


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: ☒ The ACM Digital Library ☐ The Guide


 Searching within **The ACM Digital Library** for: secure processor ([start a new search](#))

 Found **3,271** of **277,885**
REFINE YOUR SEARCH
[Search Results](#)
[Related Journals](#)
[Related Magazines](#)
[Related SI](#)

Results 1 - 20 of 3,271

 Sort by

▼ **Refine by Keywords**

Discovered Terms

▼ **Refine by People**

[Names](#)

[Institutions](#)

[Authors](#)

[Editors](#)

[Reviewers](#)

▼ **Refine by Publications**

[Publication Year](#)

[Publication Names](#)

[ACM Publications](#)

[All Publications](#)

[Content Formats](#)

[Publishers](#)

▼ **Refine by Conferences**

[Sponsors](#)

[Events](#)

[Proceeding Series](#)

[Save results to a Binder](#)

 Result page: [1](#) [2](#) [3](#)

- 1** [Making secure processors OS- and performance-friendly](#)
 Siddhartha Chhabra, Brian Rogers, Yan Solihin, Milos Prvulovic
 March 2009 **Transactions on Architecture and Code Optimization (TA)**
Publisher: ACM [Request Permissions](#)
 Full text available: Pdf (1.04 MB) [Additional Information: full citation, abstract](#)
Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 216, Download

In today's digital world, computer security issues have become increasingly important. In this paper, we present the AEGIS secure processor architecture. In this paper, we present the AEGIS secure processor architecture that utilizes hardware and integrity verification to protect the privacy ...

Keywords: Secure processor architectures, memory encryption, memory

- 2** [Design and Implementation of the AEGIS Single-Chip Secure Processor Functions](#)
 G. Edward Suh, Charles W. O'Donnell, Ishan Sachdev, Srinivas Devadas
 June 2005 **ISCA '05: Proceedings of the 32nd annual international symposium on computer architecture**
Publisher: ACM
 Full text available: Pdf (288.96 KB) [Additional Information: full citation, abstract](#)
Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 106, Download

Secure processors enable new applications by ensuring private and authentic face of physical attack. In this paper we present the AEGIS secure processor RTL implementation on FPGAs. By using ...

Also published in:

 May 2005 **SIGARCH Computer Architecture News** Volume 33 Issue 2

- 3** [Authentication Control Point and Its Implications For Secure Processors](#)
 Weidong Shi, Hsien-Hsin S. Lee
 December 2006 **MICRO 39: Proceedings of the 39th Annual IEEE/ACM International Symposium on Microarchitecture**
Publisher: IEEE Computer Society
 Full text available: Pdf (619.30 KB) [Additional Information: full citation, abstract](#)
Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 46, Download


Secure processor architecture enables tamper-proof protection on software

ADVANCED SEARCH
[Advanced Search](#)
FEEDBACK
[Please provide us with feedback](#)

 Found **3,271** of **277,885**

security problems such as reverse-engineering prevention, trusted computing environment ...


4 [Processor virtualization for secure mobile terminals](#)

 [Hiroaki Inoue, Junji Sakai, Masato Edahiro](#)

July 2008

Transactions on Design Automation of Electronic Systems

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (1.53 MB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 24, Downloads (12 Months): 234, Downloads

We propose a processor virtualization architecture, VIRTUS, to provide applications and virtualized domains for downloaded native applications generation mobile terminals can provide ...

Keywords: Multiprocessor, processor virtualization

5 [Efficient Memory Integrity Verification and Encryption for Secure Pro](#)

[G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas](#)

December 2003

MICRO 36: Proceedings of the 36th annual IEEE/ACM International Microarchitecture

Publisher: IEEE Computer Society

Full text available:  Pdf (307.01 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 79, Downloads

Secure processors enable new sets of applications such as commercial protection, and secure mobile agents by providing security from both physical and software. This paper proposes new hardware mechanisms for memory ...

6 [Using Address Independent Seed Encryption and Bonsai Merkle Tree OS- and Performance-Friendly](#)

[Brian Rogers, Siddhartha Chhabra, Milos Prvulovic, Yan Solihin](#)

December 2007

MICRO '07: Proceedings of the 40th Annual IEEE/ACM International Microarchitecture

Publisher: IEEE Computer Society

Full text available:  Pdf (954.09 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 50, Downloads

In today's digital world, computer security issues have become increasingly important. Researchers have proposed designs for secure processors which utilize hardware and integrity verification to protect the privacy ...


7 [Fast Secure Processor for Inhibiting Software Piracy and Tampering](#)

[Jun Yang, Youtao Zhang, Lan Gao](#)

December 2003

MICRO 36: Proceedings of the 36th annual IEEE/ACM International Microarchitecture

Publisher: IEEE Computer Society


Full text available:  Pdf (258.88 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 89, Downloads

Due to the widespread software piracy and virus attacks, significant effort is required for computer systems. For stand-alone computers, a key observation is that any component is vulnerable to security attacks. ...

8 [Design of secure cryptography against the threat of power-attacks in](#)

 Catherine H. Gebotys

February 2004 **Transactions on Embedded Computing Systems (TECS)**

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (214.56 KB)


Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 79, Downloads (24 Months): 12

Embedded wireless devices require secure high-performance cryptographic algorithms and low energy dissipation. This paper presents for the first time a design method for a complex DSP-embedded processor core. Elliptic ...

Keywords: VLIW

9 [A novel secure wireless video surveillance system based on Intel IXI](#)

 Hao Yin, Chuang Lin, Berton Sebastien, Xiaowen Chu

October 2005 **WMuNeP '05: Proceedings of the 1st ACM workshop on Wireless multimedia network performance modeling**

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (399.19 KB)


Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 51, Downloads (24 Months): 12

This paper presents the design of a novel high-secure wireless video surveillance system based on the 802.11g ad-hoc wireless infrastructure; and the Intel IXP420 the basic processing unit. A media-dependant ...

Keywords: ad-hoc network security, network processor, video selective

10 [Fault-secure algorithms for multiple-processor systems](#)

 Prithviraj Banerjee, Jacob A. Abraham

January 1984 **ISCA '84: Proceedings of the 11th annual international symposium on computer architecture**

Publisher: ACM

Full text available:  Pdf (844.91 KB)

Additional Information: [full citation](#), [abstract](#)


Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 35, Downloads (24 Months): 12

In this paper we describe techniques for achieving fault secureness with multiple-processor systems. In order to do this we consider the relationships between algorithms and hardware.

Also published in:

June 1984 **SIGARCH Computer Architecture News** Volume 12 Issue 3

11 [Accelerating memory decryption and authentication with frequent validation](#)


 Weidong Shi, Hsien-Hsin S. Lee

May 2007 **CF '07: Proceedings of the 4th international conference on Computer fault-tolerant design**

Publisher: ACM  [Request Permissions](#)

Full text available:

Additional Information: [full citation](#), [abstract](#)


 [Pdf](#) (336.57 KB)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 40, Download

This paper presents a novel architectural technique to hide fetch latency and authenticated memory. A number of recent secure processor design encryption and authentication to protect un-trusted ...

Keywords: message authentication, secure processors, value prediction

12 [HIDE: an infrastructure for efficiently protecting information leakage \(](#)

 [Xiaotong Zhuang, Tao Zhang, Santosh Pande](#)

December 2004 **ASPLOS-XI**: Proceedings of the 11th international conference on programming languages and operating systems

Publisher: ACM  [Request Permissions](#)

Full text available:  [Pdf](#) (216.31 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 72, Download

XOM-based secure processor has recently been introduced as a mechanism resistant execution. XOM provides support for encryption/decryption and XOM nor any other current approach adequately ...

Keywords: address bus leakage protection, secure processor


Also published in:

November 2004 **SIGPLAN Notices** Volume 39 Issue 11

December 2004 **SIGOPS Operating Systems Review** Volume 38 Issue 5

December 2004 **SIGARCH Computer Architecture News** Volume 32 Issue 5

13 [Extending hardware based mandatory access controls for memory \(](#)

 [Brian L. Sharp, Gregory D. Peterson, Lok Kwong Yan](#)

May 2008 **CSII RW '08**: Proceedings of the 4th annual workshop on Cyber intelligence research: developing strategies to meet the cyber challenges ahead

Publisher: ACM

Full text available:  [Pdf](#) (31.86 KB)


Additional Information: [full citation](#), [appendix](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 246, Download

Current memory architectures do not practice the principle of least privilege memory to data corruption and usurpation threats, collectively called memory famous of such threats is probably the buffer ...

Keywords: data corruption, data usurpation, hardware, mandatory access safety

14 [A low-cost memory remapping scheme for address bus protection](#)

 [Lan Gao, Jun Yang, Marek Chrobak, Youtao Zhang, San Nguyen, Hsien-Hsi](#)

September 2006 **PACT '06**: Proceedings of the 15th international conference

compilation techniques

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (536.42 KB)


Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 25, Downloads (24 Months): 25

The address sequence on the processor-memory bus can reveal abundance of a program. This can lead to critical information leakage such as encryption keys. Addresses can be observed by attaching ...

Keywords: address bus leakage protection, secure processor

15 AEGIS: architecture for tamper-evident and tamper-resistant processing

 G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marien van Dijk, Srinivas Aravamudan
June 2003 **ICS '03:** Proceedings of the 17th annual international conference on supercomputing

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (286.90 KB)


Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 142, Downloads (24 Months): 142


We describe the architecture for a single-chip aegis processor which can be used to secure against both physical and software attacks. Our architecture assists the processor, such as memory, ...

Keywords: certified execution, secure processors, software licensing

16 Hardware authentication leveraging performance limits in detailed simulation

 Daniel Y. Deng, Andrew H. Chan, G. Edward Suh
July 2009 **DAC '09:** Proceedings of the 46th Annual Design Automation Conference

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (197.10 KB)


Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 65, Downloads (24 Months): 65

This paper proposes a novel approach to check the authenticity of hardware. We show a performance gap between real hardware and simulations or emulations. We demonstrate that each processor design can ...

Keywords: hardware authentication, secure processors

17 A combined hardware and software architecture for secure computing

 Jürg Platte, Edwin Naroska
May 2005 **CF '05:** Proceedings of the 2nd conference on Computing frontiers

Publisher: ACM  [Request Permissions](#)

Full text available:  Pdf (507.25 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 60, Downloads (24 Months): 60

Remote code execution becomes more and more important as can be seen in computing projects like SETI@home. However, executing programs on insecure hardware poses risks if the program contains sensitive data or ...

Keywords: certified execution, encrypted programs, secure processors

18 [Hardware-rooted trust for secure key management and transient trust](#)



Jeffrey S. Dvoskin, Ruby B. Lee

October 2007 **CCS '07**: Proceedings of the 14th ACM conference on Comput

Publisher: ACM [Request Permissions](#)

Full text available: Pdf (520.62 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 137, Downl

We propose minimalist new hardware additions to a microprocessor chip portable computing devices which are used in the field but owned by a *architecture* has trust rooted ...

Keywords: emergency response, hardware policy enforcement, key ma secure processors, transient trust

19 [Architecture for Protecting Critical Secrets in Microprocessors](#)



Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dvoskin, Zhengf

June 2005 **ISCA '05**: Proceedings of the 32nd annual international sympo

Publisher: ACM

Full text available: Pdf (143.62 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 101, Downlo

We propose "secret-protected (SP)" architecture to enable secure and c secrets for a given user in an on-line environment. Keys are examples c and management is a fundamental problem ...

Also published in:

May 2005 **SIGARCH Computer Architecture News** Volume 33 Issue 2

20 [Architectural Support for High Speed Protection of Memory Integrity Multiprocessor Systems](#)

Weidong Shi, Hsien-Hsin S. Lee, Mrinmoy Ghosh, Chenghual Lu

September 2004 **PACT '04**: Proceedings of the 13th International Conferen Compilation Techniques

Publisher: IEEE Computer Society




Full text available: Pdf (255.33 KB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 65, Downloa

Recently there is a growing effort in both the architecture and the secur solution for authenticating system memory.As shown in the previous wc authentication will become a vital component for ...

Result page: [1](#) [2](#) [3](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#) 